REMARKS/ARGUMENTS

Claims 1, 14, 18, and 25 are amended herein. Claims 1-28 are currently pending.

The courteous telephone interview granted applicants' undersigned attorney by Examiner Karen Tang on July 10, 2007 is hereby respectfully acknowledged. Proposed amendments to the claims to overcome the rejections under 35 U.S.C. 112 were discussed. The rejections under 35 U.S.C. 103 were also discussed. The arguments presented in the interview are set forth below. In the interview, the Examiner stated that she was not prepared to respond to the arguments. Therefore, another interview is requested after the Examiner has had an opportunity to review the arguments and reference cited.

Claims 1, 14, 18, and 25 have been amended to clarify that a first server is located within the virtual private network and a second AAA server is associated with a gateway and not located within the virtual private network. As amended, claims 1, 14, 18, and 25 are believed to comply with the requirements of 35 U.S.C. 112.

Claims 1-10, 12-17, and 25-28 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Publication No. US 2002/0010865 (Fulton et al.) in view of Applicant Admitted Prior Art (AAPA).

Fulton et al. disclose a method and apparatus for remote office access management. A remote user 100 dials a number associated with a remote office access server to establish a connection between the user and the remote office access server (Fig. 1). User identification information is passed from the remote office access server to a security server 130, which authenticates the user information. If access is granted, the security server returns the authentication decision to the remote access server and data is permitted to pass between the user and the customer network (LAN) 150. Fig. 2 illustrates details of the remote office access manager network 110 of Fig. 1. The remote office access manager network includes a remote office access manager security server 178 which is used for AAA (see, paragraphs 0027 and 0031-0032).

Fulton et al. do not disclose providing authentication in a virtual private network (or local area network) by sending a request to authenticate a remote user to an AAA server located within the virtual private network (or local area network) that the user wants to establish a connection with. In contrast to applicants' invention, Fulton et al. disclose AAA traffic flow to a server located within a remote office access manager network, which is in communication with a local area network (LAN). As described at paragraph [004] and [0025] and illustrated at Fig. 1, a remote user 100 utilizes a dial-up connection to access a local area network (LAN) 150. The authentication process is described at paragraph [0025]. The remote user 100 first connects to ROAM network 110. The ROAM network 110 is connected to a network 120, which is connected to a security server 130 and a network routing element 140. The security server 130 examines the user information from the remote user 100 and verifies access to network 150. If authenticated by server 130, network 120 passes the data to network routing element 140 for routing to customer network 150. Fulton uses a conventional AAA server which is associated with a gateway or network that the remote user accesses in order to request access to a remote network.

Claim 1 requires, inter alia, receiving a request from a remote user for connection with a virtual private network (VPN) at a virtual home gateway, sending a request to authenticate the remote user with the VPN from the gateway to a first AAA server located within the VPN, and connecting the remote user to the VPN if the first AAA server authenticates the user. In contrast to applicants' invention, Fulton et al., send a request to authenticate a remote user 100 with a customer network 150 to an AAA server which is not located within the customer network. The AAA server is associated with the ROAM network 110. Claim 1 specifically requires that authentication of the remote user is performed without contacting a second AAA server, which is not located within the network that the remote user is trying to contact (i.e., customer network 150).

Furthermore, since the authentication is not performed at the LAN to which the remote user wants to establish a connection with, there is no need to associate the remote user with the LAN to perform authentication. In rejecting the claims, the examiner refers to Table 1 and paragraph [0038] of Fulton et al. as teaching associating a remote user with a customer network. Table 1 simply shows user specific permanent virtual circuits (PVCs)

from remote office access network 110. For example, PVC#1 extends from the network 120 to the customer network 150 and is used for communication between the remote user and customer network after the remote user has been authenticated by network 120. PVC#2 extends from ROAM network 110 to security server 130 and PVC#3 extends to a backup security server. It is PVC#2 and PVC# 3 that handles AAA traffic. PVC#1 leading to the customer network does not handle AAA traffic.

Conventional systems, such as described in the background of the invention require either that the SP maintain a complete and up-to-date database of all the remote users of each customer in order to perform complete authentication of the customers' remote users, or use the SP AAA server to contact a customer AAA server and respond back to the gateway with authorization. An important drawback to this approach is that it requires the SP AAA server and the customer AAA server to communicate, which can pose a serious security risk. Furthermore, it requires routes to be redistributed (e.g., exported, imported, and filtered) between a customer routing table and a SP routing table so that the two servers can communicate. The route redistribution is a rather complex operation that is prone to configuration errors.

In a sincere effort to expedite prosecution, claim 1 has been amended to specify performing a lookup for the address of the first AAA server at the virtual home gateway. Since none of the cited references use a gateway to directly contact a customer AAA server, there is no database relating to customer AAA servers at a gateway, and no reason to perform a lookup to find an address.

Claim 1 has been further amended to specify sending accounting information directly to the first and second AAA servers. Conventional gateways can only send accounting records to a single group of AAA servers that are reachable via a global routing table. As previously described, if a customer wants to receive accounting records for remote users, a copy of the records sent to the SP AAA server must be obtained directly from the SP AAA server. The process of proxying accounting records suffers from the same drawbacks discussed above for proxy authentication through the SP AAA server.

Applicants' invention, as set forth in the claims, is particularly advantageous in that authentication of a remote user with a VPN is performed at the VPN. This eliminates

the need for a service provider to maintain a complete and up-to-date database of all the remote users of each customer, as is required in networks such as disclosed in Fulton et al. and eliminates direct communication between a SP and VPN server.

Accordingly, claim 1 is submitted as patentable over Fulton et al.

Claims 2-13, depending either directly or indirectly from claim 1, are submitted as patentable for at least the same reasons as claim 1.

Claims 2 and 3 are further submitted as patentable over Fulton et al., which do not show or suggest receiving a virtual private network ID and address of an AAA server of the virtual private network. As discussed above, the remote user is not associated with a virtual private network and the AAA server is not located within a virtual private network.

Furthermore, claim 3 requires the virtual private network ID to bind a profile of the virtual private network to a routing table of the virtual home gateway. In rejecting claim 3, the Examiner refers to paragraphs 0025 and 0070 of Fulton et al. Paragraph 25 describes how a network routing element, separate from the remote office access network and customer network is used for routing to an appropriate customer network (see Fig. 1). Thus, there is no need to bind a profile of the customer network to a routing table of the remote office access network.

With regard to claim 6, Fulton et al. do not route an authentication request using a customer routing table in the customer network. As discussed above, the routing information is not obtained from the customer network. Thus, claim 6 is submitted as patentable over Fulton et al. and the AAPA.

Claims 8, 9, and 10 are further submitted as patentable over Fulton et al. which do not disclose sending an accounting request to the customer network. Also, Fulton et al. do not send different accounting information to a virtual private network's AAA server and service provider's AAA server, as set forth in claim 10.

Claim 14 is directed to a computer program product for providing authentication in a virtual private network having an AAA server and is submitted as patentable for at least the reasons discussed above with respect to claim 1.

Claims 15-17, depending directly from claim 14, are submitted as patentable for at least the same reasons as claim 14. Claim 17 is further submitted as patentable for the reasons discussed above with regard to claim 3.

Claims 11 and 18-24 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fulton et al. in view of U.S. Patent Publication No. 2002/0075844 (Hagen).

As noted by the Examiner, Fulton et al. do not teach identifying a virtual private network based on a domain name.

Hagen discloses a system and method for integrating public and private network resources for optimized broadband wireless access. A network access server is associated with each wireless, radio frequency communication device and provides an interface between the wireless, mobile terminals and the private network. Hagen does not remedy the deficiencies discussed above with respect to the primary reference. Furthermore, Hagen does not show or suggest associating a remote user with a virtual private network by identifying the virtual private network based on a domain name, as set forth in claim 11. In contrast to using a domain name to identify a virtual private network, Hagen discloses using the same wireless domain name for all WAP-containing networks (paragraph 0049). Thus, Hagen teaches away from associating a remote user with a specific virtual private network by using a domain name to identify the desired virtual private network.

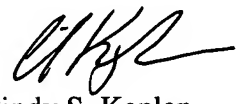
With regard to claim 18, the Examiner notes that Fulton et al. do not teach a processor operable to look up the address of the virtual private network AAA server based on information received from the remote user. In rejecting claim 18, the Examiner refers to paragraphs 0061 and 0175 of Hagan. Paragraph 0061 describes a NAS integrated in a wireless phone. Paragraph 0175 describes a registration process which involves verifying information provided on a registration form by a subscriber. A NAS is used to verify fields entered by a user on a registration form. After completing the registration process data is transmitted to the NAS. There is no teaching of a processor operable to look up the address of a virtual private network AAA server based on information received from a remote user.

Accordingly, claim 18 is submitted as nonobvious over Fulton et al. and Hagen. Claims 19-24, depending either directly or indirectly from claim 18, are submitted as patentable for at least the same reasons as claim 18.

Claim 25 is a system claim corresponding to the method of claim 1 and is submitted, along with dependent claims 26-28, as patentable for the reasons discussed above with respect to claim 1.

For the foregoing reasons, Applicants believe that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a telephone conference would in any way expedite the prosecution of the application, please do not hesitate to call the undersigned at (408) 399-5608.

Respectfully submitted,



Cindy S. Kaplan
Reg. No. 40,043

P.O. Box 2448
Saratoga, CA 95070
Tel: 408-399-5608
Fax: 408-399-5609